

J 4/12/06

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	631	(380/28).CCLS.	USPAT; USOCR	OR	OFF	2004/07/01 20:28
S2	252	(380/29).CCLS.	USPAT; USOCR	OR	OFF	2004/07/01 20:20
S3	755	(380/30).CCLS.	USPAT; USOCR	OR	OFF	2004/07/01 20:20
S4	18	(random randomly) adj (transform)	USPAT	OR	OFF	2004/07/01 20:35
S5	2	whitening adj key	USPAT	OR	OFF	2004/07/01 20:39
S6	4	(encrypt encryption) and (random adj transformation)	USPAT	OR	OFF	2004/07/01 20:43
S7	220	((("xor" "exclusive-or") same random) and (des (data adj encryption adj standard)))	USPAT	OR	OFF	2004/07/01 20:52
S8	5	((("xor" "exclusive-or") same random) and (des (data adj encryption adj standard))) and ((power adj dissipation) (signal adj (emitted fluctuation)))	USPAT	OR	OFF	2004/07/01 20:56

EAST Search History

S9	97	("6157720" "5343530" "4817140" "5734721" "4504900" "5713042" "6230182" "4319079" "4433207" "5940846" "4578535" "4894814" "6192129" "6243470" "5351299" "5454039" "5675652" "5835597" "6061449" "6061449" "6144743" "6076162" "6173402" "6253193" "6363488" "6389402" "6427140" "4283599" "4315101" "5241598" "4386266" "4914697" "4864494" "5225664" "5337357" "5561767" "6715079" "5781635" "5999628" "4829569" "4890321" "6212281" "6212281" "5412729" "5539827" "5365589" "5724428" "5481613" "5835600" "5870470").pn. ("4295039" "5195136" "6049608" "6125185" "6125182" "3798360" "4802217" "4910776" "4934846" "4969188" "5003596" "5295188" "5297208" "5351293" "5548648" "5673318" "5694473" "5757913" "5784462" "5809148" "5832087" "5835604" "5920627" "5974144" "5995623" "6014442" "6038317" "6047069" "6078663" "6151676" "6249582" "6259789" "6269164" "6307938" "6345098" "6434699" "6463150" "6490353" "6502135" "6504930" "6618761" "5754647" "6292868" "4853884" "4458109" "5201000" "5818738" "5963644" "6118869").pn.	USPAT	OR	OFF	2004/07/01 21:33
S10	5	("4319079" "4322576" "4850019" "5003597" "5261033").PN.	USPAT	OR	OFF	2004/07/01 21:04
S11	0	(random adj (transform transformation)) and (differential adj cryptanalysis)	USPAT	OR	OFF	2004/07/01 21:34
S12	75	differential adj cryptanalysis	USPAT	OR	OFF	2004/07/01 21:34
S13	5	("4319079" "4322576" "4850019" "5003597" "5261033").PN.	USPAT	OR	OFF	2004/07/01 21:42
S14	19	"5351299".URPN.	USPAT	OR	OFF	2004/07/01 21:42
S15	10	cryptanalysis and (leaked leak)	USPAT; EPO; JPO; DERWENT	OR	OFF	2004/07/02 08:47

EAST Search History

S16	13	("4908038" "5297207" "5401950" "5727063" "5778074" "5812669" "5835599" "5838795" "6041412" "6049613" "6064724" "6064740" "6069954").PN.	USPAT	OR	OFF	2004/07/02 08:43
S17	5	cryptanalysis and (timing adj (attack attacks))	USPAT; EPO; JPO; DERWENT	OR	OFF	2004/07/02 08:57
S18	0	cryptanalysis and (power adj (attack attacks))	USPAT; EPO; JPO; DERWENT	OR	OFF	2004/07/02 08:57
S19	2	cryptanalysis and (blinding adj factor)	USPAT	OR	OFF	2004/07/02 14:00
S20	6	cryptanalysis and (blinding blind)	USPAT	OR	OFF	2004/07/02 14:00
S21	13	("4908038" "5297207" "5401950" "5727063" "5778074" "5812669" "5835599" "5838795" "6041412" "6049613" "6064724" "6064740" "6069954").PN.	USPAT	OR	OFF	2004/07/02 14:01
S22	0	("9646640").PN.	USPAT	OR	OFF	2005/03/07 16:13
S23	1	("6381699").PN.	USPAT	OR	OFF	2005/03/07 16:13
S24	13	("4908038" "5297207" "5401950" "5727063" "5778074" "5812669" "5835599" "5838795" "6041412" "6049613" "6064724" "6064740" "6069954").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2005/03/08 12:43
S25	2	whitening and cryptanalysis	USPAT	OR	OFF	2005/03/08 12:47
S26	55	whitening and crypt\$	USPAT	OR	OFF	2005/03/08 16:19
S27	1452	((380/28) or (380/29) or (380/30)).CCLS.	USPAT	OR	OFF	2005/03/08 16:19
S28	65	S27 and (@pd > "20040630")	USPAT	OR	OFF	2005/03/08 16:20
S29	1	S27 and (@pd > "20040630") and (power adj consumption)	USPAT	OR	OFF	2005/03/08 16:20
S30	83026	(power adj consumption)	USPAT	OR	OFF	2005/03/08 16:21
S31	153	(power adj consumption) and (des) and encryption	USPAT	OR	OFF	2005/03/08 16:21
S32	1	(analysis adj power adj consumption) and (des) and encryption	USPAT	OR	OFF	2005/03/08 16:23
S33	198	(713/194).CCLS.	USPAT	OR	OFF	2005/03/08 16:23

EAST Search History

S34	12	S33 and (power adj consumption)	USPAT	OR	OFF	2005/03/08 16:24
S35	61	(713/192).CCLS.	USPAT	OR	OFF	2005/03/08 16:24
S36	1	S35 and (power adj consumption)	USPAT	OR	OFF	2005/03/08 16:24
S37	27	(permut\$4 modify\$4 reorder\$4) with (order with execution with operation)	USPAT	OR	OFF	2005/09/23 17:11
S38	53	(permut\$4 modify\$4 reorder\$4) with (order with execution with operation)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/09/23 17:11
S39	6	(permut\$4 modify\$4 reorder\$4) with (order with execution with operation) and (encrypt\$)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/09/23 17:16
S40	7	(permut\$4 modify\$4 reorder\$4) with (order with operation) same (encrypt\$)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/09/23 17:30
S41	889	(power adj consumption) and encrypt	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/09/23 17:31
S42	33	analy\$3 with (power adj consumption) and encrypt	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/09/23 17:31
S43	3	("4993068" "5588059" "5850443").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2005/09/23 17:36
S44	13	("4908038" "5297207" "5401950" "5727063" "5778074" "5812669" "5835599" "5838795" "6041412" "6049613" "6064724" "6064740" "6069954").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2005/09/23 17:40
S45	1754	((380/28) or (380/29) or (380/30) or (713/192) or (713/194)).CCLS.	USPAT	OR	OFF	2005/09/23 17:41

EAST Search History

S46	82	S45 and (@pd > "20050308")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/09/23 17:43
S47	78	(obfuscat\$5) same (des (data adj encryption and standard))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/09/23 17:44
S48	78	(obfuscat\$5) same (" des " (data adj encryption and standard))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/09/23 17:44
S49	8	(obfuscat\$5) same ((data adj encryption and standard))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/09/23 17:46
S50	0	(obfuscat\$5) same (encrypt\$)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/09/23 17:46
S51	306	(obfuscat\$5) same (encrypt\$)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/09/23 17:47
S52	68	(obfuscat\$5) same (encrypt\$)	USPAT	OR	ON	2005/09/23 17:55
S53	4	(obfuscat\$5) same (cipher)	USPAT	OR	ON	2005/09/23 18:01
S54	355	rdes	USPAT	OR	ON	2005/09/23 18:01
S55	10	rdes and encrypt	USPAT	OR	ON	2005/09/23 18:25
S56	27	random with processing adj order	USPAT	OR	ON	2005/09/23 20:43
S57	42	random\$4 with (modify\$3 order\$3 permut\$5) with (execution) with operation	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/09/23 20:49

EAST Search History

S58	2	kocher.in. and unpredictable.ti.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/09/23 21:10
S59	2845	(data adj encryption adj standard) and software	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/09/23 21:11
S60	1347	(data adj encryption adj standard) and software	USPAT	OR	ON	2005/09/23 21:12
S61	11	(data adj encryption adj standard).ab. and software	USPAT	OR	ON	2005/09/23 21:16
S62	142	(software adj implementation) and (data adj encryption adj standard)	USPAT	OR	ON	2005/09/23 21:15
S63	19	(data adj encryption adj standard).ab.	USPAT	OR	ON	2005/09/23 21:24
S64	104	(data adj encryption adj standard).clm.	USPAT	OR	ON	2005/09/23 21:21
S65	1	("3962539").PN.	USPAT	OR	OFF	2005/09/23 21:21
S66	59	("3962539").URPN.	USPAT	OR	ON	2005/09/23 21:22
S67	3	(data adj encryption adj standard and software).ab.	USPAT	OR	ON	2005/09/23 21:27
S68	82	(data adj encryption adj standard) same (software with implement\$6)	USPAT	OR	ON	2005/09/23 21:28
S69	1642	random\$5 with permutation	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/24 16:21
S70	6	random\$5 with permutation adj bit	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/24 16:21
S71	54	random\$5 with permutation same des	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/24 16:41
S72	1	("5623548").PN.	USPAT	OR	OFF	2006/01/24 16:41

EAST Search History

S73	8	("5623548").URPN.	USPAT	OR	ON	2006/01/24 16:44
S74	1212	((713/192) or (713/194) or (380/28) or (380/29)).CCLS.	USPAT	OR	OFF	2006/01/24 16:45
S75	52	S74 and (@pd > "20050922")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/24 16:45
S76	1	("5623548").PN.	USPAT	OR	OFF	2006/01/26 14:54
S77	1251	((713/192) or (713/194) or (380/29) or (380/28)).CCLS.	USPAT	OR	OFF	2006/04/07 16:23
S78	39	S77 and (@pd > "20060126")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/04/07 16:51
S79	0	((scramble random\$2) with order adj execution adj operation and (encrypt\$4)).clm.	US-PGPUB; USPAT	OR	ON	2006/04/07 16:52
S80	2	((scramble random\$2) with order with execution with operation and (encrypt\$4)).clm.	US-PGPUB; USPAT	OR	ON	2006/04/07 16:52
S81	20	((scramble random\$2) with order with operation and (encrypt\$4)).clm.	US-PGPUB; USPAT	OR	ON	2006/04/10 15:33
S82	3	("5872846" "6081597" "6408075").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2006/04/07 17:13
S83	1	("6408075").PN.	USPAT	OR	OFF	2006/04/07 17:13
S84	1	("5623548").PN.	USPAT	OR	OFF	2006/04/10 13:23
S87	639	(713/193).CCLS.	USPAT	OR	OFF	2006/04/10 15:33
S88	7	("4757468" "5046095" "5058164" "5247577" "5313520" "5377264" "5892826").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2006/04/10 15:41
S89	32	power with consumpt\$4 same encrypt\$5 same random\$4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/04/10 15:42

EAST Search History

S90	21	("4203166" "4214126" "4243890" "4908038" "5136646" "5241598" "5297201" "5341423" "5369706" "5401950" "5412379" "5420925" "5544086" "5552776" "5559887" "5600324" "5633930" "5733047" "5761306" "5991415" "5995629").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2006/04/10 16:11
S91	1423	((713/156) or (713/176) or (705/64) or (705/76)).CCLS.	USPAT	OR	OFF	2006/04/12 17:02
S92	140	S91 and (@pd > "20051215")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/04/12 17:03
S93	24	("20020062281" "20020107791" "20030004876" "20030055792" "20030078844" "20030101134" "20030124978" "20030135470" "20040019564" "20040122685" "20040158532" "20040199474" "20040243517" "20040267663" "20040267664" "20040267665" "20050027543" "20050065875" "20050177521" "5708422" "5764789" "6016476" "6023682" "6789966").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2006/04/12 17:06

JK 4/12/16



[Subscribe](#) (Full Service) [Register](#) (Limited Service, Free) [Login](#)

Search: ☒ The ACM Digital Library ☐ The Guide

(random or randomize) and "order of operation" and (encrypt

THE ACM DIGITAL LIBRARY



[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Terms used random or randomize and order of operation and encrypt or encryption

Found 9,359 of 173,942

Sort results by

relevance



[Save results to a Binder](#)

Display results

expanded form



[Search Tips](#)

☐ Open results in a new window

[Try an Advanced Search](#)

Try this search in [The ACM Guide](#)

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scale ☐ ☐ ☐ ☐ ☐

1 [Breaking and provably repairing the SSH authenticated encryption scheme: A case](#)



[study of the Encode-then-Encrypt-and-MAC paradigm](#)

Mihir Bellare, Tadayoshi Kohno, Chanathip Namprempre

May 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7

Issue 2

Publisher: ACM Press

Full text available: [pdf\(404.99 KB\)](#) Additional Information: [full citation](#),